Lecture 2
Network Threats

CS3690 Network Security
Summer Quarter, 2000
C. Irvine

Objectives

- Attack Thresholds
- Types of Attack
- Examples
- Targets

Attack Terminology

- Vulnerabilities
  - ★ weaknesses in system
  - ★ security flaws
  - ★ does not include benign failure
- Attacks
  - ★ exploitation of vulnerabilities
- Threats
  - ★ adversaries capable of mounting attacks against vulnerabilities
  - ★ leads to *Threat Model*
- Risk
  - ★ likelihood that vulnerability will be exploited

Need for Network Security

"The resources necessary to conduct a cyber attack are commonplace. A personal computer and a simple telephone connection to an Internet Service Provider anywhere in the world are enough to cause a great deal of harm" --PCCIP

- Attractive Targets
- Lack of Security
- Multiple user communities sharing common networks
  - ★ public networks
  - ★ common-user networks

Trends Affecting Computer Security

- Increased Interconnection to unknown users
- Use of Networks for Sensitive Information
- Soon: Ubiquitous use of Digital Signatures
- Banking - electronic funds transfer
  - ★ 1970s: electronic funds transfer -- insure integrity of transactions
  - ★ 1980s: ATM machines
    - insure secrecy of PINs across network
  - ★ 1990s: Seek cost savings using electronic services
    - want to insure authenticity of transaction
- Electronic Business Data Interchange (EDI)
  - ★ Requirements for integrity, confidentiality, authenticity
  - ★ Also need to treat as contractual documents
- Telecommunications
  - ★ Managed using networked computers
  - ★ Must protect from theft of service
  - ★ Considered critical and must have continuous operation
- Government information SBU
  - ★ need to insure privacy, e.g. electronic tax returns
  - ★ government contracts
    - Comptroller General Decision in 1991 permits government use of electronic signatures for contracts
- Corporate Proprietary Information
  - ★ contracts, proprietary information
  - ★ huge intranets connected to Internet
  - ★ increased telecommuting
  - ★ Internetworking Classified and Unclassified Networks

Application Environment Security Requirements I

- Banking
  - ★ Insure integrity of transactions
  - ★ Authenticate sources of transactions (e.g. retail transactions customers)· Insure secrecy of PINs
  - ★ Provide customer confidentiality
- Telecommunications
  - ★ Protect user's privacy
  - ★ Insure continuity of service
  - ★ Isolate administrative privileges
- Government(SBU)
  - ★ Protect Privacy Act Information
  - ★ Insure information confidentiality for SBU
  - ★ Provide electronic signatures for contractual documents

Application Environment Security Requirements II

- Government(Classified)
  - Protect information affecting national security
  - Protect intelligence information
  - Insure integrity of weapons systemsCorporate Networks
  - Protect corporate confidentiality
  - Insure authenticity of messages
- Electronic trading
  - Authenticate source of transactions
  - Insure integrity of transactions
  - Insure confidentiality of critical corporate information
  - Provide legally binding contracts

Network Security Objectives

- Confidentiality
  - Ensure that unauthorized individuals are denied access to information and resources
- Integrity
  - Ensure that information is created, modified, or destroyed only by authorized users, that data is consistent
- Availability
  - Ensure that access to information and resources are accessible to legitimate users
- Network Security
- Security measures include activities ranging from emanations security through personnel security
- Here we will concentrate on communications security and computer security
  - These must work together
    - Computer Security - security within the computer
    - Communications Security - security of information while it transits between computers
- Network security is characterized by security services
- Basic Security Notions
  - Security Policy
  - Threats and Safeguards
  - Security Services
  - Intrusion Detection and Audit Supports

Security Policies

- Apply to specific security domains and are established by authorities for those domains.
- Security policy refinement
  - Security policy objectives
    - organization's statement of intent regarding protection of specific resources. This may be quite general. For example, Government protects information that affects the national security
  - Organizational security policy
    - specific rules and regulations that describe how the security policy objectives will be achieved. An organizational security policy is often in terms of people and information. Philosophical Question: In the Information Age, do we envision policies that would not involve people?
  - System security policy
    - If we understand systems to be an extension of the people associated with the organization, then systems are operated on behalf of those people. Here the policy is a technical statement describing how a system is engineered to support the organizational security policy.

Key Aspects of Policy

- Authorization
- Access Control
  - Mandatory
  - Discretionary
- Accountability
  - Auditing
    - Identification and Authentication

Threats and Safeguards

- Threat
  - Danger to confidentiality, integrity or availability
- Passive
  - monitoring traffic
  - obtaining the contents of a message
  - traffic analysis
- Active
  - introducing a Trojan Horse to deliberately violate policy
  - modification of information
  - fabrication of false information
  - denial of service attacks
- Malicious/Accidental
  - Spamming
  - Sending e-mail to the wrong person

Threats correspond to security objectives

- Information leakage
- Integrity violation
- Denial of Service
- (some include illegitimate use)Primary Enabling Threats
- Masquerade
- Bypass of controls
- Authorization violation
- Planting Threats
- Trojan Horse Trapdoor
- Underlying Threats
  - eavesdropping
  - traffic analysis
  - loquacious, indiscreet individuals
  - media scavenging

Trends Affecting Attacks

- Increasing Ease of Engineering an Attack
- Famous attacks
  - ★ Stoll's "wiley hacker"
  - ★ Morris Internet worm
  - ★ Government homepage graffiti
  - ★ Takedown of Midnick (release of Midnick?)
  - ★ How-to guides for attackers

Security Services: Authentication

- Provides assurances of the identity of a person or system
  - ★ photo id card - driver's license
  - ★ mother's maiden name at the bank
  - ★ entity authentication
    - Authentication of a remote party in a communications exchange
    - Who's there?
    - Needed to support access control
    - Can be used to provide data integrity authentication
    - Supports accountability
    - Identities in the audit trail
  - ★ data origin authentication
    - Originator of data item is given along with data
    - Who is sending this?
    - helps to insure the integrity of a data item

Access Control Service

- provides protection against unauthorized use or manipulation of resources
  - ★ locks and keysguards
  - ★ who can use, modify, read, destroy, and issue commands
  - ★ supports confidentiality, integrity, availability
    - who can issue management commands
    - who can tie up resources
    - who can obtain information to be used for denial of service attacks

Reference Monitor Concept Critical

Reference Monitor Concept

- Mediates access
- Defines security perimeter
- POLICY INDEPENDENT
  - ★ applicable to a variety of policies
  - ★ applicable to many implementations of policy
- General Schema:
  - ★ Objects
    - passive entities containing information
  - ★ Subjects - active entities.
  - ★ Authorization Database
  - ★ Two Types of functions
    - Authorization functions - change authorization database
    - Reference functions - access information
      - observe and/or modify
- Requirements
  - Completeness Isolation Verifiability

Non-repudiation Service

- Provides protection to one or both parties in an information exchange against subsequent denial of that exchange by the other party
  - ★ notary's signature
  - ★ process servers, certified mail, receipts of mail delivery
  - ★ Repudiation of origin
    - disputes over whether a particular entity originated a given data item
  - ★ Repudiation of delivery
    - dispute over whether a particular data item was delivered to a particular party

Security Services Data Integrity Service

- Provides protection against unauthorized the modification, deletion or substitution of information
  - ★ indelible ink
  - ★ credit card/driver's licence holography
  - ★ wish to prevent: modification, replay, creation, deletion of data items - What are some banking examples?
  - ★ Granularity:
    - connection integrity service
    - connectionless integrity service
    - selected field integrity service

Security Services: Confidentiality Service

- Provides protection against unauthorized disclosure of information to entities
  - ★ opaque envelopes, seals
  - ★ invisible ink
  - ★ note the difference between data and information
  - ★ data item in storage· existence or non-existence of data item· size of data item
  - ★ dynamic characteristics of the system
  - ★ Data Confidentiality Service
    - sensitive information cannot be revealed by inspecting the size of content of a data item (encryption)
  - ★ Granularity
    - connection confidentiality service - all data transmitted on a connection
    - connectionless confidentiality service - all data in one connectionless data unit-selective field confidentiality service - applies to specific fields in the data unit
  - ★ Traffic Flow Confidentiality

Example Threats

- Informal RequirementsThreats
- Everyone: keep out hackers
- Masquerade
  - ★ Banking
    - Insure integrity of transactions
  - ★ Authenticate sources of transactions (e.g. retail transactions customers)
  - ★ Insure secrecy of PINs
  - ★ Provide customer confidentiality
- Integrity violations
- Masquerade, repudiation

Eavesdropping

- Government (SBU)
  - ★ Protect Privacy Act Information
  - ★ Insure information confidentiality for SBU
  - ★ Provide electronic signatures for contractual documents
- Masquerade, authorization violation, eavesdropping, integrity violation
- Repudiation
- Government (Classified)
  - ★ Protect information affecting national security
  - ★ Protect intelligence information
  - ★ Insure integrity of weapons systems
- Masquerade, authorization violation, eavesdropping, integrity violationCorporateProtect corporate confidentialityInsure authenticity of messages
- Eavesdropping
- Masquerade, Integrity violation
- Electronic Trading
  - ★ Authenticate source of transactions
  - ★ Insure integrity of transactions
  - ★ Insure confidentiality of critical corporate information
- Provide legally binding contracts
- Masquerade

Eavesdropping

- Repudiation
- TelecommunicationsProtect user's privacy
- Insure continuity of service
- Isolate administrative privileges

Eavesdropping

- Denial of Service
- Masquerade, authorization violation

Threat Model

- Adversary
  - ★ Sponsorship
    - State or Large Well Funded Organization
  - ★ Time
  - ★ Equipment and Resources
  - ★ Skill
  - ★ Egoless

Threat Model

- Method of Attack
  - ★ Subvert Systems During Development
  - ★ Subvert Systems During Upgrades
  - ★ Subvert Systems via Data Driven Attacks
    - Usually using the victim as an unwitting accomplice
- With Hooks in Systems
  - ★ Attack at will Any Time, Any Place

When is Security Good Enough?

- Perfect Security Cannot be Achieved
  - ★ Wouldn't want it anyway - cannot get work done
- Need security sufficient for accepted threat model
- Absence of obvious insecurity does not imply a secure system
  - ★ Dijkstra stated that there was no way other than good engineering to build sound software. Testing can demonstrate the presence or absence of a particular bug but cannot show the absence of bugs in general.
- Risk Analysis
  - ★ Permits application of Security mechanisms in a systematic manner
  - ★ Provides a methodolgy for defining Adequate Security

Attack Thresholds

- Attacks are esoteric only for a short time
  - ★ tool kits become available with tested attack tools
  - ★ inexperienced attackers can use them
- Technical Attacks are not Expensive
  - ★ hardware is relatively inexpensive
  - ★ software is effectively free
- No attack should be dismissed because it seems "too technical" for attackers

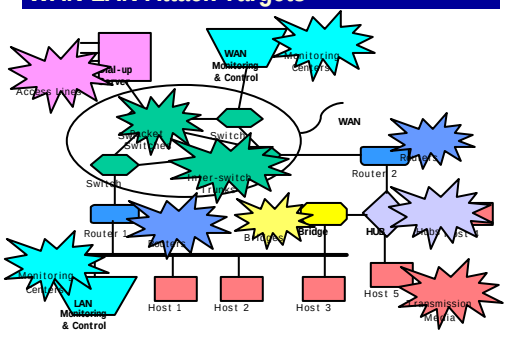
Attacks on the Wire

- Passive
  - ★ listen without modification of messages
    - do not affect network operations
  - ★ Usually cannot detect
  - ★ Preventable
- Active
  - ★ Modification of messages
  - ★ Disruptive activity
  - ★ Detectable
  - ★ Not preventable

Attacks

- Observation of Information
  - ★ impact on confidentiality
  - ★ engage in traffic analysis
- Modify Message
  - ★ change contents in manner undetectable by recipient
- Masquerade
  - ★ pretend to be someone else
- Message Stream Manipulation
  - ★ change sequence of messages
  - ★ cause delays in message recipt
  - ★ Denial of Service
  - ★ overload hosts or network, thus disrupting ability to communicate
- Replay
  - ★ reuse messages at a later time for disruptive purposes

WAN-LAN Attack Targets



Security Services

- Confidentiality
- Authenticity
- Data Integrity
- Access Control
- Non-Repudiation
- Availability

Services for Data Confidentiality

- Data is not revealed or available to unauthorized individuals, entities or processses
- Foremost objective: protection against unauthorized disclosure
  - connection-oriented confidentiality
  - connectionless confidentiality
  - selective field confidentiality
- Secondary objective: Traffic Flow security
  - patterns of message origin and destintation
  - message size
  - message transmission frequency
- Mechanisms
  - Cryptography

Services for Authenticity

- Data origin authenticity
  - who is the source of this data?
  - Needed as input for access control and audit
  - Tied to data integrity services
- Peer entity authentication
  - timeliness vs. replay
  - peer in the association is the one claimed
  - applicable to connection-oriented communication
- Granularity Considerations
- Mechanisms:
  - Key distribution
  - protocols
  - user identity validation

Data Integrity Services

- Insure against unauthorized data modification or destruction
- Connectless Integrity
  - per message
  - protect message contents from undetected modification
  - associated with data origin authentication
- Connection-oriented integrity
  - often provided by transport layer protocols
  - ensure that all of the data is at destination
    - reassembly
- Mechanisms
  - detection codes
  - time stamps
  - sequence numbers
  - cryptography

Access Control Services

- Prevent unauthorized use of resource
  - Also use in an unauthorized manner
  - Service Dependent
  - May use labels
- Policy

	Identity Based	Rule Based
User Managed	DAC	
Admin Managed	DAC*	MAC

*e.g. Packet filters based on Source Address

- Mechanisms
  - key distribution
  - cryptography
  - capabilities
  - ACLs
  - Firewalls and other "gatekeepers"

Non-Repudiation Services

- Prevent one party in a communication from denial of having participated
- Origin non-repudiation
  - Prevent false denial of having sent message
    - includes time
- Receipt non-repudiation
  - Prevent false denial of having received a message
    - includes time (what about network latency?)
- Mechanisms
  - Digital Signatures
  - Time stamps
  - Trusted software
  - Notarization

Availability Services

- Not a standard service
  - Recent DOS attacks indicate that it is needed
- Subjective
  - One person's sufficient availability may be DOS for another
- Similar to wiretapping
  - Know when it is happening
  - Cannot prevent it
- Mechanisms
  - replication and fault tolerance
  - reliability mechanisms
  - robust algorithms
    - (see Oakley later on in course)

Summer Quarter, 2000 C. Irvine; NPS CISR 37